#11

Received
FEB 13 1997

IBM International Business Machines Corporation

Office of the CHQ Export Regulation Office

1301 K Street, N.W., Washington, D.C. 20005-3307

February 12, 1997

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20230

Subject: Comments on Federal Register Notice dated December 30, 1996
Encryption Items Transferred From the U.S. Munitions List
to the Commerce Control List

Dear Ms. Crowe:

In response to the above Federal Register notice, we have the following comments. Please note that IBM may have additional, policy related comments, that would be communicated to the Department of Commerce in a separate letter.

We would like to express our general concern that many of the ITAR restrictions were, with this regulation, ported into the EAR. Of a specific concern are the regulations regarding publicly available technology and software, new definition of export and the exclusion of GSN for EI controlled items. Introduction of these rules appears to be contrary to the recent liberalization of export controls.

Background Section:

Reference is made to November 15, 1996 as the final date under which encryption items could have been transferred from Department of State USML to Department of Commerce CCL controls. We believe that the date is actually December 30, 1996, not November 15.

Key Recovery Agents

There are several references throughout the regulation referring to one recovery agent for a key recovery product. In case of IBM, the key recovery encryption products will be based on SKR which will support multiple key recovery agents.

The key recovery agents that may be used by a key recovery encryption product can be independent of the key recovery encryption product. There is no need for the product or the vendor of the product to know the names of the key recovery agents used by the product.We can provide further technical information; however, for the purpose of these comments, we request that the regulations allow for flexibility for use of different technologies that manufacturers will implement.

This comment is also applicable to Supplement No. 5 to Part 742 - Key Escrow or Key Recovery Agent Criteria.

Replacement of Department of State Personal Use Exemption (PUE) by license exceptions TMP and BAG.

We very much appreciate the simplification of the rules for hand carrying cryptographic products and clarifying that license exceptions TMP and BAG will replace the PUE. However, license exceptions TMP and BAG need to be amended as follows:

TMP: Definition of 'Tool of Trade' needs to be expanded for countries in group D1

BAG: the requirement that the items must be owned by the individual needs to be eliminated

734.2 - Definition of Export - (b)(9)(ii)(A)

We propose that, in case the software is made available on an Intranet of a U.S. or Canadian company (i.e. available only within the U.S. or Canadian company), item (1) of the regulatory requirement for checking that requests are only coming from the United States be eliminated.

For other than Intranet requests we suggest that the requests can be coming from either the United States or Canada since export licenses are not required for products destined for use in Canada.

734.4 (h)

In view of the fact that there will be bi-lateral agreements on encryption with other countries, and in order to streamline the process, we are proposing the following to be added:

' In countries with which the US Government has a bi-lateral encryption agreement, the government shall permit, without further approval, for key recovery products to lose their U.S.origin when redrawn,used, consulted, or otherwise commingled abroad in any respect with other software or technology of any other origin.'

We believe that it is in the interest of the US Government to proliferate key recovery technology worldwide. This addition would also help US manufacturers to compete, without obstacles, with foreign competitors in the area of key recovery products and technology.

740.8 - Key Management Infrastructure

(d)(E) For clarity, 'Key holding obligations' needs to be defined here or a reference made to what it meant by the obligations.

(e) Reporting requirements
Since there will be no limitation on customers who will be eligible to obtain 56 bit DES products under this license exception, we are proposing that this requirement be eliminated. The elimination would greatly ease the administrative burden on the exporters. If the elimination cannot be achieved, we request that the reporting is only of the exporter's customer which may or may not be the ultimate consignee. It is not possible to report ultimate consignees for mass marketed products or OEM (Other Equipment Manufacturer) customers.

742.15 Encryption Items

We request that the rule be amended to authorize exporters to follow Department of Commerce rules on Destination Control Statements as well as rules on filing Shippers Export Declarations (SED) for all encryption items now under the jurisdiction of the Department of Commerce. It would streamline the process and alleviate administrative burden. In the case of IBM it would allow us to file automatic monthly reports for products exported under license exception KMI as well as those exported under the Distribution Arrangement (DA) previously approved by the Department of State. It would also allow us to have one destination control statement for all encryption products, not one for KMI and another for the DA.

(4) All other encryption items
We propose that a license exception be issued for encryption items subject to EI controls with the key of less than 56 bit. Otherwise, 56 bit DES product could be exported under a license exception while a 40 bit product would require a license.

Supplement No.4 to Part 742-Key Escrow or Key Recovery Products Criteria

(2) We recommend to replace the portion of the first sentence which reads 'The product's cryptographic functions shall be...' with the follbwing words:
'The product's cryptographic functions supporting the key recovery feature shall be.....'

(6) (i)
We request that this paragraph be deleted or modified. The party that conformed with the requirements stated in this regulation would have to have means to detect that other party's system had been altered. This appears to add complexity to the key recovery protocol that is, in our opinion, unnecessary and may not even be possible to accomplish.

(8)
The described method is just one possible way to achieve the objective. Escrowing the 'keys or other material' with a key recovery agent is but one possible way to ensure that law enforcement, with a warrant or court order, can recover the 'keys or other material' and

then decrypt the ciphertext. There are other possible ways in which this can be accomplished. For instance, one part is held by the key recovery agent and the other part is appended as a header to the encrypted data or stored with the encrypted data. The regulation should allow flexibility to use different technologies.

Supplement No. 5 to Part 742 - Key Escrow or Key Recovery Agent Criteria

The regulation stipulates that the key recovery/escrow agents will have to be named by December 31, 1998. It is our understanding that a recovery agent cannot be named overseas until a bi-lateral agreement is reached between the United States and the applicable country. Since our overseas customers may require that the agents be located in their countries, rather than in the United States, we are emphasizing the urgency that is required on the part of the US Government to complete the bi-lateral agreements before then, at least for the OECD countries.

I. Key Recovery Agent Requirements
We feel very strongly that the obligations be placed only on a company, not on individuals. Certifications and information on individuals would add a significant burden on the administration and add additional time for processing. All these additional expenses add to the cost of the final product.

II. Security Policies
References are made several times to 'database'. We propose to change that to 'information relevant to key recovery or key escrow'.

Supplement No. 6 to Part 742 - Guidelines for Submitting a Classification Request for a Mass Market Software

We propose that '512' bit key be replaced with '1024' bit key for key management for 40 bits algorithms as well as for 56 bit DES. The increased length key management would add credibility to these products, especially in view of the recent articles about the ease of breaking 40 bit algorithms.

(c) In order to clarify for exporters what other algorithms they can use, we propose to change the first sentence as follows:
'Instructions for the preparation and submission of a classification request for products implementing the CDMF (Commercial Data Masking Facility) or other approved algorithms that are eligible for 15 day handling as follows:....'

774

'Note 5D002 Does Not Control' statement must include the anti virus software. Previously the anti-virus software was eligible for license exceptions TSR and CIV. This was omitted from the December 30, 1996 interim rule. In addition, the anti-virus software is no longer controlled under the Wassenaar Arrangement. Therefore, it should be classified as EAR99 or 5D995.

The regulation should also specify whether Trusted Systems B2 or lower fall within the classification of EAR99, 5A995 or 5D995.

The Statement of the Vice President (dated October 1, 1996) referred to future special treatment for financial applications, a practice that had already been in place.The Statement stated that 'Longer key lengths will continue to be approved for products dedicated to the support of financial applications'. The regulations do not address this provision and a clarification is necessary so that companies can build products for financial applications that are exportable. Special treatment also needs to be given to US and Canadian subsidiaries for their internal use.

We also propose that the category 5 (Information Security) of the CCL (Commerce Control List) be amended to include products that comply with SET requirements and that these are automatically eligible for license exceptions TSR or GBS or are classified under ECCN 5D995 or 5A995.

In summary, we would like to thank you for the opportunity to comment on the interim regulation and hope that our comments will be reflected in the final rule. We would like to emphasize that IBM supports the spirit of the key recovery idea but we would like to minimize the administrative requirements that increase the cost of the products without providing significant benefits.

Sincerely,

W. D. Koshner
Corporate Director of Export Licensing